# Getting Started with RFID

chapter 1

in this chapter

- ☑ Introducing RFID
- ☑ Using RFID
- ☑ Understanding RFID basics

*RFID* or *Radio Frequency Identification* is used throughout the world. It's mostly leveraged by big business, but that's changing. It's becoming a technology well within reach of the everyday hobbyist. Unfortunately, the majority of RFID books you'll find on shelves today mostly deal with the process of implementing RFID throughout businesses large and small, for the purpose of inventory management, personnel management, and supply chain automation. Other books about RFID contain every piece of technical information you could ever want to know regarding radio energy theory and signal propagation. This book is not about either of these things.

The purpose of this book is to introduce enthusiastic, project-hungry gadgetiers everywhere to the concepts of RFID and make the point that this technology isn't just for big business — you can build great projects on a hobbyist's budget.

The approach taken with this book is one based on concepts and components. You may notice several projects centered on the same basic idea of access control, but the point of each project is to present solutions using different available components, or show different ways to overcome project-specific challenges. The idea is to give a good selection of RFID based projects you can build, while at the same time conveying the concepts involved so you can choose to either duplicate the projects shown in this book, or come up with your own RFID solutions.



## What Is RFID?

As mentioned at the beginning of this chapter, RFID stands for Radio Frequency Identification. The name perfectly describes the purpose of this technology: to identify something using radio signals.

## Early RFID — IFF

One of the first widespread systems to use radio signals for identification was the *IFF* (Identification Friend or Foe) system first developed and used by the British during World War II. From there it was further developed into the RFID-based technology currently used by air traffic controllers everywhere. Its design was developed around radar signals, so the IFF system was easily adapted and integrated with aircraft track control systems. The IFF system went through several generations, but each generation used radar signals to interrogate an aircraft and receive identifying information back from that aircraft.

## RFID Tags and Interrogators

RFID is a two-part system including interrogators and tags. The interrogators are the "readers" and the tags are the pieces that store the information. Compared to a barcode system, the barcode scanner is like the reader and the barcode label itself is like the RFID tag.

RFID tags come in a variety of shapes, styles, and sizes designed to suit a particular need. Figure 1-1 shows some of the different types of tags available, including access cards, printed labels with embedded RFID tags, RFID key chains (sometimes called *keyfobs*), and so on.

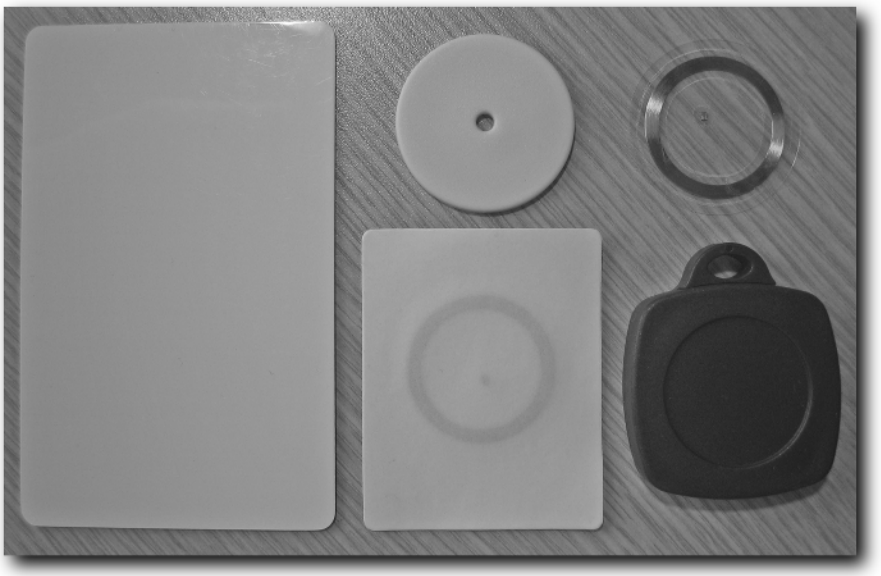

**Figure 1-1: Various types of RFID tags**

# Contemporary Uses of RFID

Since the IFF system, RFID has slowly crept into society, seemingly undetected. Many people don't realize that the anti-theft systems that now guard many storefront entryways and exits use RFID technology, or that the access cards people pass over sensors to get in and out of security doors everyday are RFID devices.

The *EAS* or *Electronic Article Surveillance* systems seen in stores typically use a simple bit tag like the one shown in Figure 1-2, which can only represent two states: 1 or 0, on or off. So really, the EAS system is basically looking for presence. The system is asking, "Is there a tag present in my field that has not been switched off by the counter clerk?" If so, an alarm sounds.

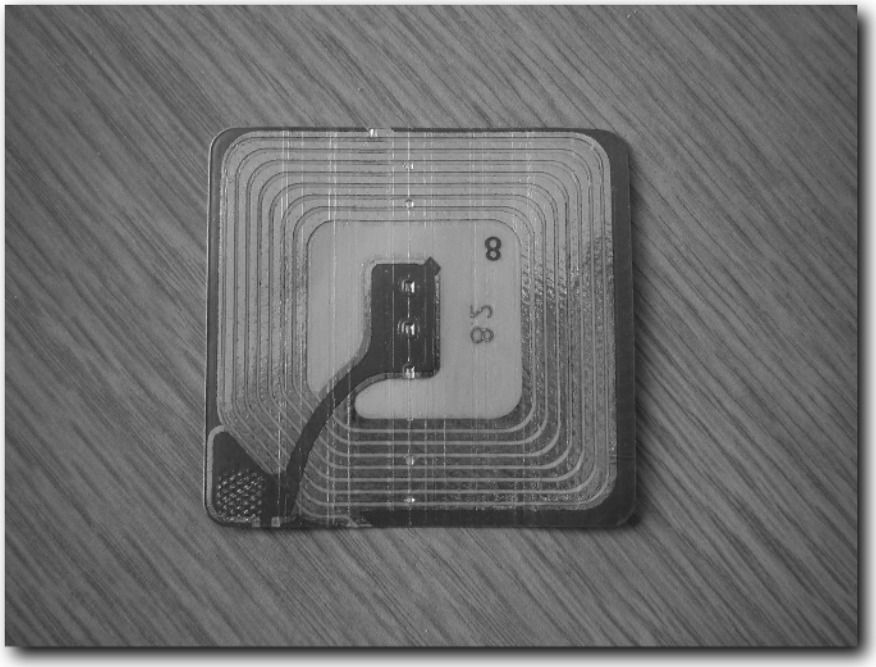

**Figure 1-2: EAS label type RFID tag**

A much more complicated system employs RFID tags to track inventory, the scope of which could range all the way from the manufacturer, through the shipping and distribution process, right down to retail shelves. Unlike barcodes and UPC codes, which label only a type of inventory with a specific number (like 1234 for oranges and 5678 for apples), RFID can assign each item (each orange and each apple) its own serial number, and track each item.

Let's take a look at a piece of clothing — a sweatshirt, for example. The idea is that supply chains and inventory could be tracked and managed from the moment the shirt was sewn together, through shipment to a distribution house, to resellers, and all the way to sitting on the shelf in some storefront. With the advent of "smart shelves," real-time inventory tracking is now possible. A simple query can actively scan the store that instant to reveal the exact number of blue sweatshirts sitting on shelf B254 in store 19301. With that kind of visibility, region managers could shuffle inventory around between stores according to demand in an area instead of simply ordering more sweatshirts while a store 5 miles away has plenty sitting on the shelf.

The idea of tracking people has been around a long time, but until recently there just wasn't enough social tolerance or technical capability to implement these types of systems. People viewed the possibility of being tracked as an egregious and oppressive intrusion into their personal privacy, even on the job. Over the last decade or so, privacy concerns have waned and RFID has been used to track employees via RFID-enabled badges, implement access control and personnel tracking for Mexican government officials implanted with RFID transponders, and track prisoners wearing RFID tracking bracelets throughout prison complexes. This type of technology is on a rapid ascent. It's being used to track the attendance and, in some cases, the location and movement of people, animals, and things.

Some rather interesting and innovative uses for RFID have been creeping into the mainstream lately. Casinos now use the same RFID technology in their betting tables that stores use to track inventory on their shelves. With betting chips that contain RFID tags, casinos now have unprecedented visibility of the floor. For instance, the dealer can know exactly what amount is on the table and where the bets are placed. The table itself knows automatically if more bets are placed after being waved off, or if chips are removed or stolen. This information is relayed back up to the security room to be combined with camera information so a security officer watching a table can see what's happening and get backup data from the RFID system in the table to confirm his or her observations.

Medical schools and universities are now tagging, of all things, cadavers. Apparently, cadaver theft is a big problem and by tagging cadavers in random places, unauthorized removal of the cadaver is immediately caught and reported.

# RFID Basics

A few basic things can define RFID: standards; data access, encoding, and transmission (air interface protocol); power source; and frequency.

## RFID Standards

There are several RFID standards in place, covering many different aspects like frequencies and data-encoding methods as well as specific uses of RFID technology such as animal tracking (ISO 11784/11785). There are also countless proprietary implementations of RFID systems (tags, readers, and software) used for various purposes, including pet "chipping" and registration. While there are ISO standards-based solutions intended for animal identification, there are three or four proprietary systems made by companies like AVID, Destron, Trovan, and others. These proprietary chips all use their own air interface (method for communicating between tag and reader) and require special reader hardware made by the same company as the tag. But,

it may be possible to find hardware made by other manufacturers that has the ability to read these proprietary tags. Just don't count on it being cheap.

At first, there was no set of rules in place that standardized on a frequency that was internationally friendly and a data encoding and transmission method (called the *air interface*) for RFID that was compatible across various tags and readers. RFID systems were all based on the same basic ideas and concepts, but manufacturers were creating their own reader and tags that were essentially proprietary. Eventually some tag standards came along, but they only governed certain aspects like frequency or air interface, leaving manufacturers to continue to create their own proprietary tags and readers. On one hand, this allowed manufacturers to innovate and give their products a competitive edge. On the other hand, it created an RFID industry filled with incompatible devices and tags that used frequencies that were not permissible in other countries.

In December 2004, the non-profit group EPCglobal Inc. submitted the high frequency (UHF) RFID Generation 2.0, or "RFID Gen 2" standard to the ISO standards committee. If it's approved, it would mean UHF tags and readers using Gen 2 would be cross compatible, and the frequency used would not break regulatory law in the various countries around the world using RFID Gen 2. The end result is that an RFID tag affixed to a shipping crate in the United States will work properly with readers when it gets to the United Kingdom, regardless of tag and reader manufacturer. Lack of international standards has been a major roadblock to smooth global deployment and intercontinental use of RFID technology thus far.

## Data Encoding and Transmission

Tags are the heart of RFID systems. They store the data, which enables the entire point of the system: identification. How this data is stored, accessed, changed, and transmitted over the air is different based on the maker of the tag. There are a few standards in place, but the fact is that many manufacturers of RFID equipment have come up with their own methods of storing data on RFID tags and developed their own protocols for reading, writing, and transmitting that data. There are several types of data encoding and access methods out there such as EM4102 from EM Microelectronic, ISO 14443, ISO 15693, HiTag from Philips, and many others. Some support security measures, while others are open to any reader within range.

Table 1-1 shows a quick cross-section of the types of RFID technologies out there, their uses, and their typical read ranges.

**Table 1-1 RFID Frequencies, Uses, and Typical Range**

| *Frequency* | *Use* | *Pros and Cons* | *Range* |
|---|---|---|---|
| 125 KHz – 148 KHz | | | |
| Type: Passive | Animal tracking (ISO 11784/ 11785), access control, and OEM applications. | Signal negotiates liquids and metals fairly well. Higher tag cost due to long length solid copper antennas. | ½" to 4" is typical. 6" to 12" or more may be possible with specialized equipment. |

*Continued*

**Table 1-1** ***(continued)***

| *Frequency* | *Use* | *Pros and Cons* | *Range* |
|---|---|---|---|
| 13.56 MHz | | | |
| Type: Passive | EAS (anti-theft), book and document management, access control, and OEM applications. | Antennas can be printed on substrate or labels, lowering tag costs. Serious interference from metals. | Can range from inches to several feet depending on reader hardware and tag type. |
| 433 MHz (and 2.5 GHz) | | | |
| Type: Active | Highway toll payment systems, vehicle/fleet management, asset tracking, and so on. | Very long range. Very high tag cost. Uses a battery, so tags have a finite lifespan (typically 5 years). | Typically around 30 feet, but can range up to hundreds of feet. |
| 915 MHz | | | |
| Type: Passive | Supply chain tracking and OEM applications. | Very low cost tag. Long range. Anti-collision capabilities allow simultaneous tag reads. Serious interference from liquids and the human body. | About 10' from a single antenna and 20' between two antennas. Longer ranges can be realized with special hardware. |

# Project Preparations

Before you begin the projects in this book, you should be aware of the security and safety issues involved.

## Security

The projects in this book are meant to be cheap, easy, and fun. But they use tags and readers that are open format. There are inherent security risks involved as these tags can be read by anyone with the right reader. The IDs stored on each tag are unique, but can be duplicated onto another tag, or an entire tag can be spoofed as well, given the right kind of equipment and software. Keep this in mind when implementing your own RFID projects and solutions.

There are secure RFID options available, but it costs quite a bit more for this kind of hardware. However, even secure tags like the ones used for Exxon Mobile's SpeedPass quick payment system have already been easily compromised, as shown at `www.rfidanalysis.org`.

While the RFID projects in this book may not seem secure to some readers, you may want to think about your security concerns in a different context. If you build an RFID-enabled front door for your home, consider what a person who wanted to break in would rather do. Would they want to sneak up on you, get a reader within 2" of your RFID tag, duplicate your RFID tag ID and break in that way, or would they rather just walk up and break your window?

## Safety

There will be a lot of cutting and soldering and other various activities that could potentially harm you in some manner or fashion. Please use common sense, and if you're unable to handle hot soldering irons or sharp cutting implements without cutting yourself or burning your house down, get someone who can handle these kinds of things to help you out.